Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

Live Object for Securing Graphical Passwords

Pooja Kale[1], Ankita Pansare[2], Vikky D. Jambhulkar[3]

[1]Computer Department, P K Technical Campus,Chakan

[2]Computer Department, P K Technical Campus,Chakan

[3]Assistant Professor, Computer Department, P K Technical Campus,Chakan

Abstract --- To apply more safety to the cloud system, Live Object for a securing graphical password is a new graphical watchword scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical tokens, here in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users represent these images to a system camera and then enter their password as a sequence of selections on live video of the toke. The reliability study shows that image feature based passwords are viable and suggests appropriate system thresholds password items should contain a minimum of seven features, 40 percent of which must match originals stored on an authentication server in order to be judged equivalent. The usability study measures task completion times and error rates, revealing these to be 7.5 and 9 percent, broadly comparable with prior graphical password systems that use static digital images.

Keywords- ORB, SIFT, Pass-BYOP, Cloud, Security,PINs

I. INTRODUCTION

Secure access to information underpins modern digital systems and services. We keep our communications, financial data, work documents, and personal media safe by providing identity information and then authenticating to that identity. Text passwords and personal identification numbers (PINs) are the dominant authentication method as they are simple and can be deployed on systems including public terminals, the web, and mobile devices. In now a days Cloud data storage and access is fully based on the text passwords or the pin codes, which is not a good way to secure the cloud data. Because text passwords or the pin codes are the easily guessable thing by shoulder surfing. To overcome this problem we propose a new way to get the access to cloud data storage and access. In that we are going to use the Image processing concept for login purpose.

However, watchwords suffer from limitations in terms of memorability and security passwords that are difficult to guess are also hard to remember. This is a major problem as an average user possesses 25 online accounts secured with up to six different passwords and representing a substantial memory burden. To deal with this problem, individuals adopt non secure coping strategies such as reuse of passwords across systems, noting down passwords, or simply forgetting them entirely . In order to mitigate these problems, researchers have proposed graphical password schemes , that rely on input such as selecting portions of an image.

II. RELATED WORK

Graphical watchword systems are knowledge based authentication techniques that leverage peoples ability to memorize and recognize visual information more readily than alphanumeric information [9]. Researchers have explored three broad types of graphical passwords: recall based drawmetric schemes based on sketching shapes on screen, recognition-based cognometric schemes based on selecting known items from large sets of options, and cued recall locimetric schemes based on selecting regions of prechosen images [3],[7]. Locimetric schemes are discussed as is multifactor

authentication, as it relates to Pass-BYOP and its combination of a token, or something you have, on which a password, or something you know, is entered.

IV. PROPOSED SYSTEM

In Proposed System, We are using ORB algorithms to dynamic size selection of image to get proper object of image. we are provide cloud log-in process security and Selected file store securely on cloud storage or in database storage to provide secure user authentication. ORB Image comparison algorithm is used compare image for log-in process. In that ,we store one sample face image and password as the same image on cloud storage.Face detection and recognition algorithm is used compare faces. ORB can be used in computer vision tasks like object Recolonization or 3D Reconstruction. It is based on the Fast Key Point Detector and the visual descriptor BRIEF (Binary Robust Independent Elementary Features). Its aim is to provide a fast and efficient alternative to SIFT Oriented FAST and Rotated BRIEF is a very fast binary descriptor based on BRIEF,which is rotation invariant and resistant to noise. It can be demonstrated through experiments how ORB is at two orders of magnitude faster than SIFT, while performing as well in many situations. The capability is tested on real-world applications, including cross detection and patch-tracking on a smart phone.

A. Advantages of Proposed System

1) A graphical password authentication system is relatively inexpensive to implement.
2) Graphical passwords provide a way of making user friendly password.
3) Graphical password are not vulnerable to dictionary attacks.
4) It is less convenient for a user to give away graphical passwords to another person.

V. SYSTEM ARCHITECTURE

The webcam is attached to a system running Live Object for a securing graphical watchword. The Pass Bring Your own pictures interface and video feed are shown on an Apple iPad that is connected wirelessly to the PC via a screen-sharing application [see (1) in Figure] and fixed to the surface of a desk. The video resolution on the iPad is 450*600 pixels or approx-imately 8.5 cm * 14 cm. All input to the system is made on the iPad touchscreen. Specifically, as illustrated in (2) in Figure, users make selections by tapping the screen to visually highlight 70 * 70 pixel portions of the displayed image, drag to move this region and release to select it. Once an image portion is selected, it is stored as a password item and displayed as feedback to the user at the base of the screen [see (2) in Figure]. Users must input a total of four items and then press an OK button in order to enter a complete password. They can also press a reset button to clear the entered password items at any time.

In existing graphical watchword systems, the watchwords are represented as the XY image coordinates of finger selections. This technique does not work with Pass Bring Your Own Pictures as variations in image placement on the terminal camera will lead to substantial variations in the XY pixel positions of image content. Instead, Pass Bring Your Own Pictures selections are stored on the authentication server as a set of optical features computed with the SIFT image processing algorithm. This was achieved by capturing a 140 * 140 image subsection around the center point of each watchword item.

A Gaussian blur was then applied and Lowes SIFT algorithm was computed with the peak threshold set to 2 and the edge threshold set to 10. This yields a list of image features and descriptors. Those that fell outside the central 70 * 70 selection box were discarded and the remainder used for
password matching.

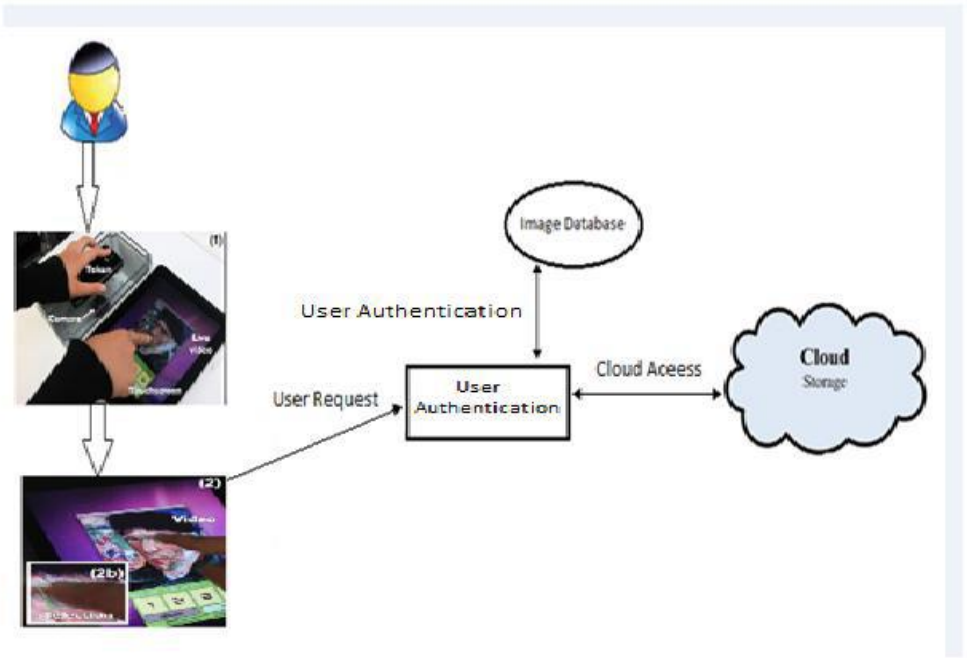

Figure 1. System Architecture

VI .METHODOLOGY

A.ORB Algorithm

i. Find the position of the key points by FAST(Features from accelerated segment test).
ii. Selecting N best points by Harris.
iii. Scale-pyramid transform.
iv. Add a direction of the points in Intensity Centroid.
v. Extracting Binary descriptor by BRIEF(Binary Robust Independent Elementary Features).
vi. Get steered brief.
vii. Find low correlative pixel blocks in greedy algorithm.
viii. Receive a 256-bit descriptor.

The required hardware for our system is as follows::

1.Processor: Pentium III, IV, V/laptop
2. Memory (RAM):2 GB
3. HDD: 20GB

The required software for our system is as follows::

1. Operating System: Windows 2007
2. Application Libraries: Base class libraries

3. Language: .java (JDK 1.8)
4. Netbeans 8.0.2
5. Oracle 10G

VII. RESULT ANALYSIS

In Figure 2. Firstly Overview of the Live Object For Securing Graphical Password system. In second diagram Input selection and closeup (2b). In third diagram Input selections that make up a password. In fourth diagram Successful authentication and In fifth diagram denied authentication. Live Object For Securing Graphical watchword is a new graphical password scheme to apply more safety to the cloud that replaces the static digital images typically used in graphical password systems with personalized physical tokens, herein in the form of digital pictures displayed on a physical user-owned device such as a mobile phone.

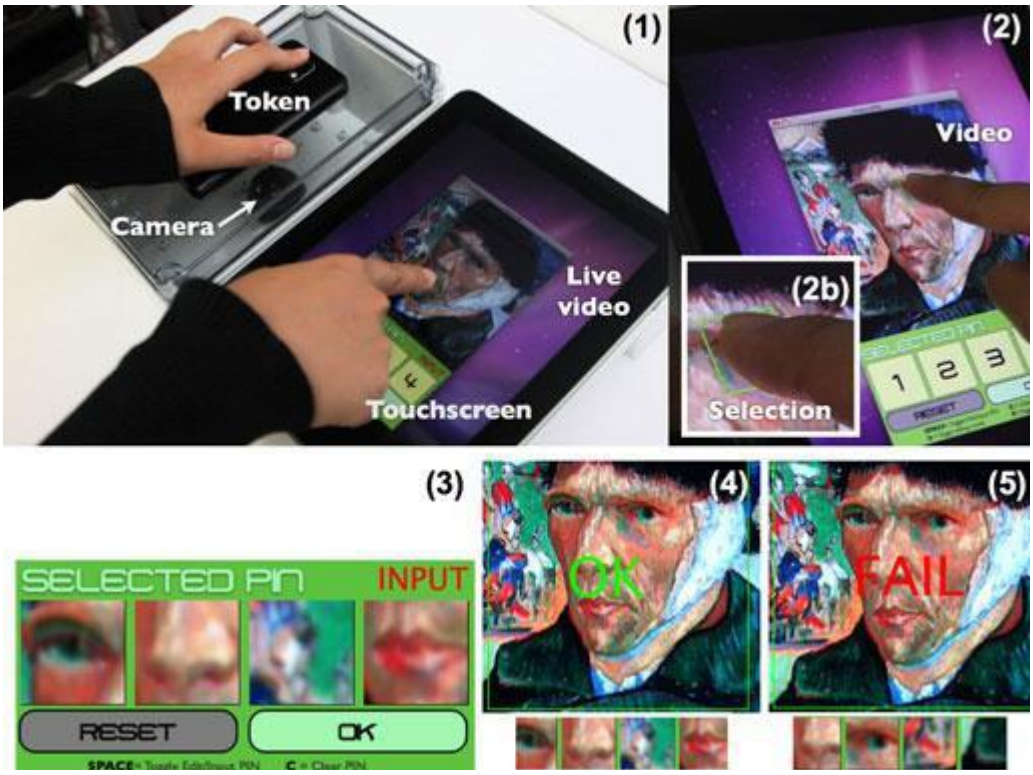

Figure 2. Result Analysis

Users must input a total of four items and then press an OK button in order to enter a complete watchword. They can also press a reset button to clear the entered password items at any time.

VIII. CONCLUSION

To improve the security of cloud access by graphical password systems by integrating live object of a physical token that a user carries with them. It first demonstrates the feasibility of the concept by building and testing a fully functional prototype then illustrates that user performance is equivalent to that attained in standard graphical password systems through a usability study assessing task time, error rate, and subjective workload. Finally, a safety study shows that live object for securing graphical password substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes.

IX. REFERENCES

[1] The A. Adams and M. Sasse,"Users are not the enemy" Commun. ACM, 1999, vol. 42, pp. 40 46.

[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack two factor authentication internet banking," in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322 328, 2013.

[3]The R. Biddle, S. Chiasson, and P. van Oorschot, Graphical passwords: Learning from the first 12 years, ACM Comput. 2012 Surveys vol. 44, no. 4, p. 19.

[4] The ARTigo, http://www.artigo.org/

[5] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using Mobile phones," Proc. Comput.Syst.Appl., 2009, pp. 641 644.

[6]B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam, Secure, consumer friendly web authentication and payments with a phone, in Proc. 2nd Int. ICST Conf. Mobile Comput., Appl., Serv., 2010, pp. 1738.

[7] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, A comprehensive study of frequency, interference, and training of multiple graphical passwords, in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009, pp. 889898.

[8] G. Lowe, Distinctive image features from scale-invariant keypoints, Int. J. Comput. Vision, vol. 60, no. 2, 91110, 2004.

[9] D. Nelson, V. Reed, and J. Walling, Pictorial superiority e_ect, J.